

11-02-00

A

PTO/SB/05 MODIFIED BY AT&T CORP.

UTILITY PATENT APPLICATION TRANSMITTAL

Attorney Docket No.	2000-0020	Total Pages	20
First Named Inventor or Application Identifier			
Craig L. DeCaluwe et al.			
Express Mail Label No.	EL618317775US		

Only for nonprovisional applications under 37 CFR 1.53(b)

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

ADDRESS TO: Assistant Commissioner for Patents
Box Patent Application
Washington, D.C. 20231

1. ☒ Fee Transmittal Form
(submit an original, and a duplicate for fee processing)
2. ☒ Specification [Total Pages 9]
(preferred arrangement set forth below)
 - Descriptive title of invention
 - Cross References to Related Applications
 - Statement Regarding Fed sponsored R&D
 - Reference to Microfiche Appendix
 - Background of the Invention
 - Brief Summary of the Invention
 - Brief Description of the Drawings(if filed)
 - Detailed Description
 - Claim(s)
 - Abstract of the Disclosure
3. ☒ Drawing(s)(35 USC 113) [Total Sheets 2]
4. Oath or Declaration [Total Pages 3]
 - a. ☒ Newly executed (original or copy)
 - b. ☐ Copy from a prior application(37 CFR 1.63(d))
(for continuation/divisional with Box 17 completed)
[Note Box 5 below]
 - i. ☐ DELETION OF INVENTOR(S)
Signed statement attached deleting inventor(s)
named in the prior application, see 37 CFR
1.63(d)(2) and 1.33(b)
5. ☐ Incorporation by reference(useable if Box 4b is checked)
The entire disclosure of the prior application, from which a copy of the oath
or declaration is supplied under Box 4b, is considered as being part of the
disclosure of the accompanying application and is hereby incorporated by
reference herein.

6. ☐ Microfiche Computer Program (Appendix)
7. ☐ Nucleotide and/or Amino Acid Sequence Submission
(if applicable, all necessary)
 - a. ☐ Computer Readable Copy
 - b. ☐ Paper Copy(identical to computer copy)
 - c. ☐ Statement verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

8. ☒ Assignment Papers(cover sheet & document(s))
9. ☐ 37 CFR 3.73(b)Statement ☐ Power of Attorney
10. ☐ English Translation Document (if applicable)
11. ☐ Information Disclosure ☐ Copies of IDS
Statement(IDS)/PTO-1449 Citations
12. ☐ Preliminary Amendment
13. ☒ Return Receipt Postcard (MPEP 503)
(Should be specifically itemized)
14. ☐ Small Entity ☐ Statement filed in prior application,
Statement(s) Status still proper and desired
15. ☐ Certified Copy of Priority Document(s)
(if foreign priority is claimed)
16. ☐ Other :

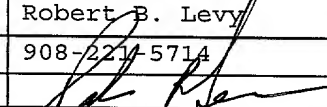
17. If a CONTINUING APPLICATION, check appropriate box and supply the requisite information:
☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior Application No:

18. CORRESPONDENCE ADDRESS

<input type="checkbox"/> Customer Number or Bar Code Label	(Insert Customer No. or Attach bar code label here)	or <input checked="" type="checkbox"/> Correspondence address below
--	---	---

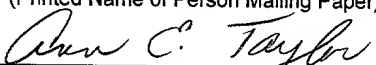
NAME	Samuel H. Dworesky				
ADDRESS	AT&T CORP. P.O. Box 4110				
CITY	Middletown	STATE	New Jersey	ZIP CODE	07748-4110
COUNTRY	United States of America			FAX	732-368-6932

19. SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

NAME	Robert B. Levy	Reg. #	28234	
TELEPHONE	908-224-5714			
SIGNATURE			DATE	Nov. 1, 2000

"Express Mail" Mailing Label Number EL618317775US Date of Deposit 11/1/2000
I hereby certify that this application is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to the Assistant Commissioner for Patents, Washington D.C. , 20231

Ann E. Taylor
(Printed Name of Person Mailing Paper)


(Signature of Person Mailing Paper)

FEE TRANSMITTAL

Patent Fees are subject to annual revision on October 1.

These are the fees effective October 1, 1997

Small Entity payments must be supported by a small entity Statement, otherwise, large entity fees must be paid. See Forms PTO/SB/09-12.

Complete if Known

Application Number

Filing Date

First Named Inventor

Craig L. DeCaluwe et al.

Examiner Name

Group/Art Unit

Attorney Docket No.

2000-0020

**TOTAL AMOUNT
OF PAYMENT**

\$710.00

METHOD OF PAYMENT (check one)

1. The Commissioner is hereby authorized to charge indicated fees and credit any overpayments to.

Deposit Account
Number 01-2745Deposit Account
Name AT&T CORP.Charge Any Additional Fee
Required Under 37 CFR 1.16
and 1.17Charge the Issue Fee Set in 37
CFR 1.18 at the Mailing Date
of the Notice of Allowance2. ☐ Payment Enclosed

Check



Money Order



Other

FEE CALCULATION**1. FILING FEE**

Large Fee Code	Entity Fee(\$)	Fee Description	Fee Paid
101	710	Utility Filing Fee	\$710.00
106	320	Design Filing Fee	
107	480	Plant Filing Fee	
108	710	Reissue Filing Fee	
114	150	Provisional Filing Fee	

SUBTOTAL (1) \$710.00**2. CLAIMS**

New Filing



Amendment

Total	8	- 20 =	Extra Claims	x	Fee from below	=	Fee Paid
			0		18		\$0.00
Ind.	2	- 3 =	0		80		\$0.00
Multiple Dependent Claims			0				\$0.00

Large Fee Code	Entity Fee(\$)	Fee Description
103	18	Claims in excess of 20
102	80	Independent Claims in excess of 3
104	270	Multiple Dependent Claims
109	80	Reissue independent claims over original patent
110	18	Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) \$0.00**3. ADDITIONAL FEES**

Large Fee Code	Entity Fee(\$)	Fee Description	Fee Paid
105	130	Surcharge - late filing fee or oath	
127	50	Surcharge - late provisional filing fee or cover sheet	
139	130	Non-English specification	
147	2520	For filing a request for reexamination	
112	920*	Requesting publication of SIR prior to Examiner action	
113	1840*	Requesting publication of SIR after to Examiner action	
115	110	Extension for reply within first month	
116	390	Extension for reply within second month	
117	890	Extension for reply within third month	
118	1390	Extension for reply within fourth month	
128	1890	Extension for reply within fifth month	
119	310	Notice of Appeal	
120	310	Filing a brief in support of an appeal	
121	270	Request for oral hearing	
138	1510	Petition to institute a public use proceeding	
140	110	Petition to revive - unavoidable	
141	1240	Petition to revive - unintentional	
142	1240	Utility issue fee (or reissue)	
143	440	Design issue fee	
144	580	Plant issue fee	
122	130	Petitions to the Commissioner	
123	50	Petitions related to provisional applications	
126	240	Submission of Information Disclosure Statement	
581	40	Recording each patent assignment per property (times number of properties)	
146	710	Filing a submission after final rejection (37 CFR 1.129(a))	
149	710	For each additional invention to be examined (37 CFR 1.129(b))	
Other fee (specify)			
Other fee (specify)			

* Reduced by Basic
Filing Fee Paid**SUBTOTAL (3)****SUBMITTED BY**Typed or
Printed Name

Robert B. Levy

Complete (if applicable)

Reg.
Number

28234

Signature

Date

Nov. 1, 2000

Deposit Account User ID

SEND TO: Assistant Commissioner for Patents, Box Patent Application, Washington, D.C. 20231

**METHOD FOR TRACKING SOURCE AND DESTINATION INTERNET
PROTOCOL DATA**

FIELD OF THE INVENTION

This invention relates to data networks. In particular this invention relates to a
5 method and an apparatus for managing data flow in an Internet Protocol (IP) network so
as to prevent network disruption caused by excessive data flow through one or more
switches.

BACKGROUND OF THE INVENTION

Figure 1 depicts a simplified block diagram of a simplified IP data network 100 of
10 the prior art. The IP network 100 allows IP data to be sent between network users 120
and 122. A network of IP routers 102, 104, 106, and 108 (the purpose, function and
operation of which are well known in the art) are interconnected by several data paths
110, 112, 114, 116, and 118 such that data from a particular customer 120 can be routed
to/from other internet protocol data network customer 122 using any pathway through the
15 network 100 such as coaxial cable, fiber optic cable, microwave data or other appropriate
links between the routers.

As an example of a pathway through the network, data from a customer 120 might
be received at a first router 108 and routed over a data path 118 to another router 102
which routes the traffic over the pathway 110 to the other router 104 connected to the
20 destination address, customer 122. Alternate pathways through the network 100 might
route data from router 108 through router 102 to router 106 and then to router 104. Yet
another pathway might exist from router 108 to 106 to 104.

A problem with an IP data network, such as the simplified depiction in Figure 1, is that one or more individual routers or internet protocol data switches can become overloaded by the transmission of data to a particular destination address or the receipt of too much data from a particular source address. Curtailing or limiting data to or through a router might limit the economic losses caused by data that is lost because a router is overloaded.

It is well known that IP data packets include both source and destination addresses, which are numerical indicators of the computer of the network from which the data originated and to which a packet is to be sent. In an internet protocol data system, misdelivered or discarded data packets that are not received by the destination are retransmitted by the source at the request of the destination when expected data packets, identified by other data transmitted with each packet, do not arrive.

Another problem with prior art internet protocol data switching networks is the inability to manage or control the flow of data from a particular source address or to a destination address in order to avoid overloading one or more routers in a network so as to insure the smooth flow of data packets through the overall network. A method and apparatus by which an internet protocol data network can manage the receipt of data from or to an address location would be an improvement over the prior art.

SUMMARY OF THE INVENTION

In an IP data network, source and destination IP addresses are recorded in memory in a router. The data on source and destination addresses of the data packets passing through the router are read through a user interface, or alternatively by a

computer, to tabulate the amount of data from and to individual IP source and destination addresses.

When the data traffic from or to a particular IP address exceeds a predetermined threshold rate, the router can be controlled to discard messages either from a particular IP address or to a particular IP address via a user interface.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 shows a simplified block diagram of a prior art internet protocol data network.

Figure 2 shows a simplified block diagram of an exemplary router device with incoming data lines, outgoing data lines and buffer and memory devices by which source and destination IP addresses are tracked and recorded.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Figure 2 shows a simplified block diagram of an improved internet protocol router 200. Incoming data lines 202, 204, and 206 carry internet protocol data packets, not shown, into the router 200; outgoing data lines 210, 212, 214 carry internet protocol (IP) data packets out of the router 200.

As is well known to those skilled in the art, IP data packets resemble Ethernet data packets in that each includes an address known as a source address that identifies a computer from which the data packet was originated. Each IP data packet also includes a destination address, which uniquely identifies the destination or end point to which the data packet is to be routed and delivered.

In Figure 2, incoming data packets, i.e., data packets arriving on incoming lines 202, 204, or 206, are received at one or more data buffers 208 within the router 200. The data buffers 208 are typically comprised of random access memory (RAM) or equivalent (perhaps an appropriate fast disk drive) and provide an elastic storage for the data packets
5 in the router device 200 that are eventually transmitted on outbound data lines 210, 212, and 214 to other points in the IP network.

While IP data packets are resident in the buffer 208 of the router 200, the source and destination IP addresses within each data packet are copied into or stored into a memory device 216, which acts to accumulate a record of the data traffic through the
10 router 200 over a finite period of time. By using the accumulated data in the memory device 216, a processor, either within the router 200 or outside the router via a user interface 220, tabulates or counts the occurrence of either or both the source addresses and destination addresses of data packets passing through the router 200.

By counting the occurrences of source addresses and/or destination addresses
15 carried through the router 200 over a predetermined time interval, the length of which is a design choice, it is possible to measure the amount of traffic to and/or from a particular IP address so as to prevent data from a particular router, such as the routers 102, 104, 106 or 108 in Figure 1, from overloading another router in the network.

By way of example, so-called computer hackers, intent on frustrating a computer
20 network, might cause massive amounts of spurious data to be generated to or from one or more other routers in the network. Large numbers of data transmission from one switch (or source address) to another switch (or destination address) might be attributable to

many causes. . (In most instances, hackers cause many switches to send data to one switch to drive it into overload.) By tracking the data origins and destinations by source and destination addresses, it is possible to prevent such acts from crippling an entire data network if overruns (sometimes referred to as storms of data or data storms) of data are
5 discarded or suppressed.

In Figure 2, a user interface 220, which provides access to the data stored in memory 216, allows the accumulated tally of source addresses and destination addresses to be manually read. If the count of source and destination addresses per unit time exceeds some predetermined threshold, commands entered by the user interface 220
10 configure the router 200 to ignore IP data packets from, or to, the problematic address.

In an alternate embodiment, data traffic volume to or from a particular source address is monitored automatically. In the unlikely event that the source switching system were to be overloaded by an overwhelming amount of data for a destination address, an intervening router can inhibit the over-loaded switch from bringing a network down by
15 overloading one or more of the intermediate nodes of the network.

In the preferred embodiment, a running count (or tabulation) of data packets received from a source address or to be sent to a destination address can be entered via the user interface 220 to the router itself 200. Alternate embodiments would certainly include substituting a computer manager for the user interface 220 such that the computer
20 manager 220 would automatically poll the memory 216 over time to monitor the rate at which packets are flowing through the router. In the event the data from a particular address or to another address exceeded some manually or automatically determined

threshold, both of which could be determined either empirically or heuristically, network congestion might be avoided by manually or automatically suppressing the reception of additional data packets from a particular source or discarding data packets accordingly.

For purposes of claim construction, the manual and automatic determination of a

5 threshold at which packets might be suppressed or discarded are considered to be equivalent. Similarly, the manual and automatic suppression of packets is considered to be equivalent.

The action of discarding a data packet can be accomplished simply by ignoring incoming data packets from a source address. Alternative methods would include

10 overriding previously stored data packets in a buffer with newly received data packets such that the end result is that the total volume of data packets from a source does not exceed some predetermined allowable threshold. One or more messages might be sent from one router to another, instructing the other switch to discard packets from a particular source. A variant of such an embodiment would include sending such an alarm
15 message throughout the network so that all switches connected therein would discard problematic data. As for the inhibition of packet transmission, an overwhelmingly large number of data packets addressed to a destination can be controlled simply by deleting or overriding outbound packets with new or other information.

By monitoring the source address data and the destination address data in an IP
20 protocol network, data overflow on a network might be avoided. By automating the monitoring and maintenance of data traffic through the network, overall system reliability can be increased.

We claim:

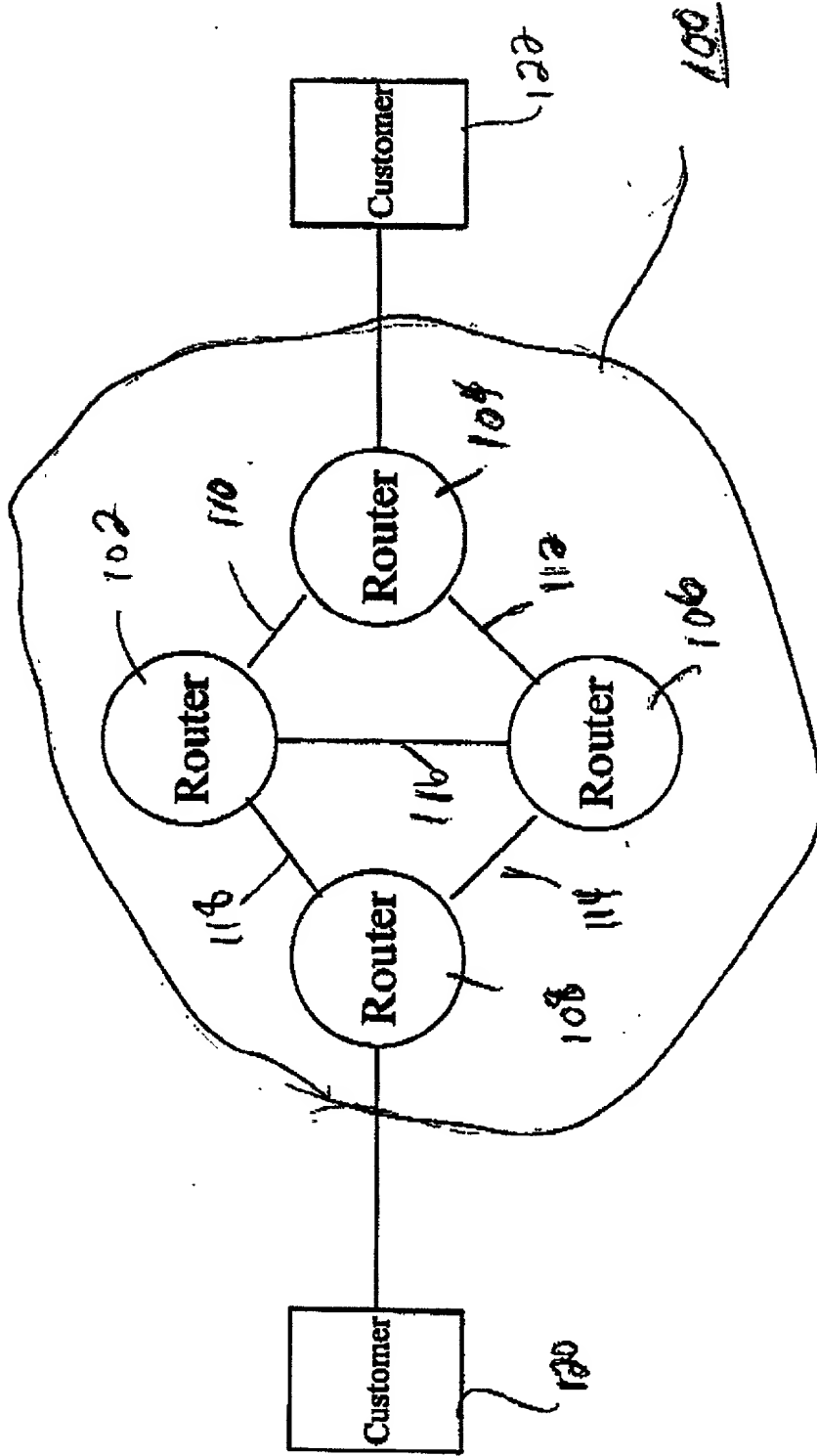
1. In an Internet Protocol (IP) data network comprised of a plurality of interconnected IP data switching systems, a method comprised of:
 - a. receiving at a first IP data switching system a plurality of IP data packets;
 - b. tabulating at said first IP data switching system at least the number of IP data packets received from a particular IP source address during a first time interval, thereby forming a count of IP data packets from a particular source;
 - c. storing said count of IP data packets in a memory device for subsequent processing.
2. The method of claim 1 further including the steps of:
 - d. reading said count of IP data packets from said memory device;
 - e. selectively discarding IP data packets received at said first IP data switching system that originated from said particular source.
3. The method of claim 1 wherein said IP data switching system is an IP data router switching system.
4. The method of claim 2 wherein said step of selectively discarding IP data packets includes the step of denying reception of IP data packets from a router based upon a source address in IP data packets upon the determination that the count of IP data packets from a source address exceeds a threshold value.

5. In an Internet Protocol (IP) data network comprised of a plurality of interconnected IP data switching systems, a method comprised of:
 - a. sending a plurality of IP data packets from a first IP data switching system to a second IP data switching system;
 - 5 b. tabulating at said first IP data switching system at least the number of IP data packets sent to a particular IP destination address during a first time interval, thereby forming a count of IP data packets sent to a particular IP destination address;
 - c. storing said count of IP data packets sent to a particular IP destination
10 address in a memory device for subsequent processing.
6. The method of claim 5 further including the steps of:
 - d. reading said count of IP data packets from said memory device;
 - e. selectively inhibiting the transmission of IP data packets from said first IP
15 data switching system to said second IP data switching system when the number of IP packets from said first IP data switching system exceeds a predetermined number.
7. The method of claim 5 wherein at least one of said first and second IP data switching systems is an IP data router switching system.
8. The method of claim 5 wherein said step of selectively inhibiting the
20 transmission of IP data packets includes the step of sending a message to a specific router to discard messages either received from or sent to a specific IP address.

ABSTRACT OF THE DISCLOSURE

In an IP network, tabulating the number of data packets received from and/or sent to a particular IP address over time can provide a mechanism by which it is possible to determine or predict overloading of a node or nodes in an IP data network. By selectively
5 deleting data packets received from a suspect source address or inhibiting the transmission of data packets to a suspect destination address, network management and control can be readily accomplished.

Typical IP Network



Prior Art

FIG. 1

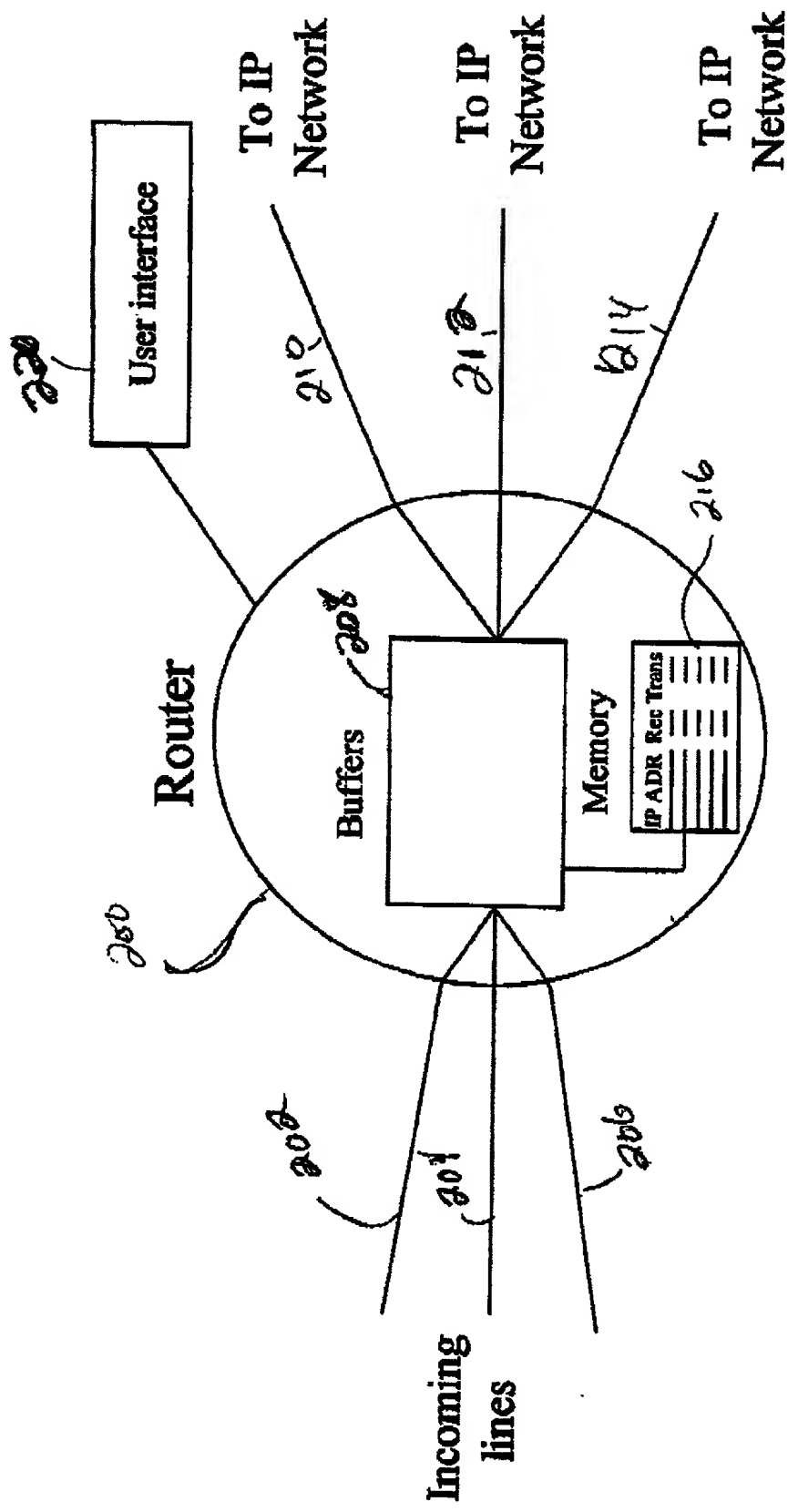


FIG. 2

IN THE UNITED STATES
PATENT AND TRADEMARK OFFICE

Declaration and Power of Attorney

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am an original, first and joint inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled **Method For Tracking Source And Destination Internet Protocol Data**, the specification of which is attached hereto.

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by an amendment, if any, specifically referred to in this oath or declaration.

I acknowledge the duty to disclose all information known to me which is material to patentability as defined in Title 37, Code of Federal Regulations, 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, 119(a-d) or 365(a-b) of PCT or foreign application(s) for patent or inventors' certificate listed below or priority benefits under 119(e) of any United States provisional application(s) listed below and have also identified below any foreign application for patent or inventors' certificate having a filing date before that of the application on which priority is claimed:

None

I hereby claim the benefit under Title 35, United States Code, 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, 112, we acknowledge the duty to disclose all information known to us to be material to patentability as defined in Title 37, Code of Federal Regulations, 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

None

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

I hereby appoint the following attorney(s) with full power of substitution and revocation, to prosecute said application, to make alterations and amendments therein, to receive the patent, and to transact all business in the Patent and Trademark Office connected therewith:

Samuel H. Dworetsky	(Reg. No. 27873)	Robert B. Levy	(Reg. No. 28234)
Thomas A. Restaino	(Reg. No. 33444)	Susan E. McGahan	(Reg. No. 35948)
Michele L. Conover	(Reg. No. 34962)	Gary H. Monka	(Reg. No. 35290)
Cedric G. DeLaCruz	(Reg. No. 36498)	Jeffrey M. Navon	(Reg. No. 32711)
Rohini K. Garg	(Reg. No. 45272)	Stephen J. Pentlicki	(Reg. No. 40125)
Thomas M. Isaacson	(Reg. No. 44166)	Alfred G. Steinmetz	(Reg. No. 22971)
Benjamin S. Lee	(Reg. No. 42787)		

I also appoint Thomas H. Jackson (Reg. No. 29808), Frederic M. Meeker (Reg. No. 35282), and Joseph P. Krause (Reg. No. 32578) of Banner & Witcoff as associate attorneys, with full power to prosecute said application, to make alterations and amendments therein, and to transact all business in the Patent and Trademark Office connected therewith.

Please address all correspondence to Mr. S. H. Dworetsky, AT&T Corp., P.O. Box 4110, Middletown, New Jersey 07748. Telephone calls should be made to Robert B. Levy at 908-221-5714.

Full name of 1st joint inventor: Craig L. DeCaluwe

Inventor's signature Craig L. DeCaluwe Date 10/25/00

Residence: Naperville, DuPage County, Illinois

Citizenship: United States of America

Post Office Address: 331 Brooklea Court
Naperville, Illinois 60565

Full name of 2nd joint inventor: Hossein Eslambolchi

Inventor's signature Hossein Eslambolchi Date 10/17/00

Residence: Los Altos Hills, Santa Clara County, California

Citizenship: United States of America

Post Office Address: 13826 Moon Lane
Los Altos Hills, California 94022